(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 109 280 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.10.2009 Bulletin 2009/42

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **08154391.0**

(22) Date of filing: **11.04.2008**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA MK RS

(71) Applicant: **Deutsche Telekom AG**
53113 Bonn (DE)

(72) Inventors:
- **Roshandel, Mehran**
  13591 Berlin (DE)
- **Goldstein, Markus**
  67655 Kaiserslautern (DE)
- **Reif, Matthias**
  67663 Kaiserslautern (DE)
- **Stahl, Armin**
  67663 Kaiserslautern (DE)
- **Breue, Thomas**
  67655 Kaiserslautern (DE)

(74) Representative: **Vossius & Partner**
Siebertstrasse 4
81675 München (DE)

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

(54) Method and system for throttling or blocking geographical areas for mitigation of distributed denial of service attacks using a graphical user interface

(57) The invention describes a method and system of protecting computer systems from attacks over a network to which the computer system is connected, the method comprising the steps of (a) monitoring current requests to the computer system; (b) measuring one or more network features on the basis of the current requests; (c) providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests; (d) receiving a user input selecting at least one geographical area; (e) accessing on the basis of the selected at least one geographical area a database associating for the at least one geographical area of origin each country with corresponding IP addresses; and (f) automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

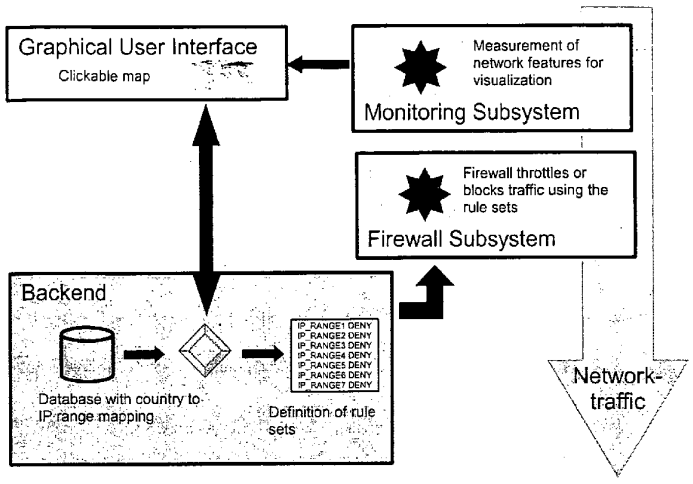

Fig. 1

EP 2 109 280 A1

Description

Field of the Invention

[0001] The invention generally relates to mitigation of Distributed Denial of Service (DDoS) attacks on public available Internet services. Examples of such services include websites, Internet telephony (VoIP), FTP server, DNS, etc.

Background of the Invention

[0002] In the Internet, Distributed Denial of Service attacks (DDoS) have become a major threat today. Large scaled networks of infected PCs (bots or zombies) combine their bandwidth and computational power in order to overload a publicly available service and denial it for legal users. All public servers are basically vulnerable to DDoS attacks due to the open structure of the Internet. The bots are usually acquired automatically by hackers who use software tools to scan through the network, detecting vulnerabilities and exploiting the target machine.

[0003] The number of such DDoS incidents is steadily increasing. For example, the attacks against large e-commerce sites in February 2000 and the attacks against root DNS servers in 2003 and 2007 have drawn public attention to the problem of DDoS attacks. Today, mainly mid-sized websites are attacked by criminals in order to extort protection money from their owners without attracting too much public attention. Besides that, also Internet Service Providers (ISP) have to deal with the problem that DDoS traffic is congesting their link bandwidths.

[0004] The bot software also evolved alarmingly over time. Early tools like *TFN, Stacheldraht, Trinoo* or *Mstream* used unencrypted and hierarchically organized communication structures. Most of these tools used TCP-SYN, UDP or ICMP floods with possibly identifiable parameters. Since some of these attacks have successfully been mitigated, a new generation of bots arose. *SDBot, Agobot* or the very enhanced *Phatbot* are known representatives which use IRC as a robust and secure communication. These tools also contain methods for spreading themselves and have more sophisticated attack algorithms, which could be upgraded over the Internet. The attack traffic from those tools looks like legal traffic on the transport layer, which makes it nearly impossible to filter it effectively with standard firewalls.

[0005] Mitigating DDoS attacks at the origin or within the core of the Internet seems to be an impossible task due to the distributed and authorization-free nature of the IP based network. Approaches to achieve this objective typically rely on changing current internet protocols and are therefore not easily applicable. Ingress filtering as described in RFC 2827 (P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," United States, 2000, available at: http://rfc.net/rfc2827.html.) also helps mitigating DDoS attacks with forged source IP addresses (IP spoofing) and should be applied by every ISP. Since ingress filtering only helps other ISPs on the Internet and not the one who is actually applying it, it took quite a long time until it was setup in many places. Furthermore, Savage et al. (S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical network support for IP traceback," in SIGCOMM, 2000, pp. 295-306) suggested IP Traceback to find the source of spoofed IP addresses by probabilistically marking packets. Nowadays, IP spoofing is not that common any more in DDoS attacks, except for the last octet of an IP address.

[0006] A known system to mitigate attacks is Radware's DefensePro with the APSolute operating system (http"//www.radwar.com/Products/ApplicationNetwork-Security/DefensePro.aspx). According to this system, the IP packets are examined for common striking features, for example identical packet sizes, source- and target ports etc. This system performs well in case of only a small number of attack sources, since attacker generate comparably high number of requests or in case of having identical attack packets.

[0007] Thus, today, there is a strong need to mitigate DDoS attacks near the target, which seems to be the only solution to the problem in the current internet infrastructure. The aim of such a protection system is to limit their destabilizing effect on the server through identifying malicious requests.

[0008] Thus, Distributed Denial of Service (DDoS) attacks are today the most destabilizing factor in the global Internet and there is a strong need for sophisticated solutions.

[0009] Typically, computer systems are protected by a security component, a firewall. The configuration of such a firewall is made via sets of rules that describe the features of incoming packets that are allowed to pass the firewall or are to be rejected. The parameters for a rule are diverse and depend on the system used. In many cases protocol, target port and source port, target and source network address and flow direction of the data packet are indicated. In the Internet, the target and source network address consists of the IP address (which is an abstract computer address) and the network mask. The rejecting or allowing-to-pass a plurality of not connected intervals requires the definition of many rules for the firewall. However, since there is no direct relationship between IP addresses and geographical location of a computer, a large number of such rules is in fact necessary to define a country, for example.

Summary of the Invention

[0010] The invention starts out from the idea of monitoring the actual requests to a computer system and preventing over load situations on the basis of information about the geographical origin of the requests with a graphical user interface (GUI).

[0011] According to a first aspect, the invention provides a method of protecting a computer system from

attacks over a network to which the computer system is connected, the method comprising the steps of (a) monitoring current requests to the computer system; (b) measuring one or more network features on the basis of the current requests; (c) providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests; (d) receiving a user input selecting at least one geographical area; (e) accessing on the basis of the selected at least one geographical area a database associating the at least one geographical area of origin each country with corresponding IP address ranges; and (f) automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area. Step a) preferably also comprises accessing the database on the basis of the monitored IP addresses to retrieve therefrom information with respect to the country the monitored request is coming from.

[0012] The method preferably comprises the further step g) of filtering a sender or requests from a sender depending on the generated firewall rules for the selected at least one geographical area. The step of filtering may comprise of a request or bandwidth throttling algorithm, wherein the limit for a particular sender corresponds to the geographical area of origin. Thus, certain requests or sender are not completely blocked. Rather, the number of accepted requests or the provided bandwidth for a particular sender or country, for example, is throttled, i.e. some requests are delayed or even denied. Technically, this corresponds to an artificial limitation of the bandwidth available for this particular sender by queuing or dropping IP packets, also known as bandwidth throttling, traffic shaping or policing.

[0013] The sum of all limits for all senders is selected on the basis of the server load or bandwidth usage of the computer system.

[0014] The measured network features is preferably selected from the group comprising: country of origin, packet rates, application features, and transmission volume, or combinations thereof.

[0015] The graphical user interface preferably comprises a geographical map. According to a preferred embodiment, the graphical user interface provides different levels of geographical maps, the levels comprising world map, continental maps, local maps, individual country maps, city maps. The measured one or more network features for each geographical area are visualized by the graphical user interface in different graphical features. For example, the graphical feature is selected from the group comprising colour, graphical pattern, flashing or combinations thereof. The geographical area is, for example, selected from the group comprising country, province, state, or city.

[0016] According to the invention, a request is preferably an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

[0017] According to a second aspect, the invention provides a system for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising: means for monitoring current requests to the computer system; means for measuring one or more network features on the basis of the current requests; display means for providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests; an input means receiving a user input selecting at least one geographical area; a database associating for the at least one geographical area of origin each country with corresponding IP addresses; and means for automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

Brief Description of the Drawings

[0018] A preferred embodiment of the invention is described in more detail below with reference to the attached drawing, which is by way of example only.

Fig. 1 shows a data flow diagram according to a preferred embodiment of the invention; and
Fig. 2 shows an example for a graphical user interface in the form of a world map.

Detailed Description

[0019] Fig. 1 shows a data flow diagram according to a preferred embodiment of the invention. As shown in Fig. 1, the system monitors the actual data traffic and measures network features with respect to geographical areas, such as countries. The measured network features are then processed for visualisation with a graphical user interface. An example of such graphical user interface will be described in detail with reference to the example shown in Fig. 2. The graphical user interface provides the user with details about the current Internet traffic and assists the user to identify attacks to the computer system. The origin of a (potential) attack can therefore easily and quickly located. With reference to the graphical user interface, the user of the computer system can select one or more geographical areas that appears to represent a threat to the computer system. Such selection causes the system to access a database that associates each geographical area, for example country, with corresponding IP addresses. On the basis of this information obtained from the database, the system automatically generates rules for the firewall as a protective measure against attacks.

[0020] According to the invention, certain requests or sender or countries are preferably not completely blocked if they are determined as being abnormal. Rather, the number of accepted requests from a country is reduced/restricted, i.e. some requests from a sender are accepted and some are rejected. This corresponds to an

artificial limitation or throttling of the bandwidth available for this particular country. The overall number of requests to be rejected or the amount of throttle bandwidth is adjustable via the graphical user interface for an administrator so that an overload is prevented.

[0021] Fig. 2 shows an example of a part of a graphical user interface in the form of a world map. With such a graphical user interface, current Internet traffic can be visualised easily and quickly for assisting the automatic generation of firewall rules. Graphical user interfaces in the form of maps can be displayed at one or more levels. The highest level is represented by a world map as shown in Fig. 2. At respective lower levels selectable by a user areas such as individual continents, individual countries, provinces or states, or even individual cities can preferably be visualized.

[0022] The visualisation provides, for example by different colouring, the user with details about network features such as Internet traffic for each geographical area, for example on a per-country-basis. The example of Fig. 2 shows a dark colouring for Russia representing a for example abnormal high traffic volume originating from Russia, wherein the U.S.A. are coloured with a brighter colour representing less abnormal traffic from there. Instead of using different colours, different graphical pattern could be used to distinguish between areas having different traffic, or the country borders could be flashing at different frequencies to provide such details for each country.

[0023] The individual colour or pattern, for example, each correspond in the map to a value of the measured network feature, such as number of requests, transmission volume, or estimated number of attacker.

[0024] According to the invention, the system waits for a user input selecting a specific geographical area, for example a specific country. Such selection may be made with a computer mouse or touchpad or other input devices pointing on the desired country on the displayed map. Such selection initiates a corresponding action in the firewall system of the computer system. For example, by selecting a specific country, this country may be completely blocked or at least the traffic originating there from may be limited. For example, a bandwidth throttling algorithm may be initiated limiting the bandwidth for the selected country to 10MBit/s. For adjusting these limitation values, further graphical user interface elements are used (not shown in Fig. 2). Thus, the computer system is still fully available for all requests coming from other countries. User from this particular country are likely not successful in accessing the requested computer system.

[0025] The present invention has now been described with reference to several embodiments thereof. It will be apparent to those skilled in the art that many changes can be made in the embodiments described without departing from the scope of the present invention. Thus the scope of the present invention should not be limited to the methods and systems described in this application, but only by methods and systems described by the language of the claims and the equivalents thereof.

Claims

1. Method of protecting a computer system from attacks over a network to which the computer system is connected, the method comprising the steps of:

   a. monitoring current requests to the computer system;
   b. measuring one or more network features on the basis of the current requests;
   c. providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests;
   d. receiving a user input selecting at least one geographical area;
   e. accessing on the basis of the selected at least one geographical area a database associating for the at least one geographical area of origin each country with corresponding IP addresses; and
   f. automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

2. The method of any of the preceding claims, further comprising the step g) of filtering a sender or requests from a sender depending on the generated firewall rules for the selected at least one geographical area.

3. The method of claim 1 or 2, wherein step a) preferably also comprises accessing the database on the basis of the monitored IP addresses to retrieve therefrom information with respect to the country the monitored request is coming from.

4. The method of claim 2 or 3, wherein the step of filtering comprises of a request or bandwidth throttling algorithm, wherein the limit for a particular sender corresponds to the geographical area of origin.

5. The method of any of the preceding claims, wherein the sum of all limits for all senders is selected on the basis of the server load or bandwidth usage of the computer system.

6. The method of claim 5, wherein the measured network features is selected from the group comprising: country of origin, packet rates, application features, transmission volume, estimated number of requests in a defined time interval, or combinations thereof.

7. The method of any of the preceding claims, wherein

in step c) the graphical user interface comprises a geographical map.

8. The method of claim 7, wherein the graphical user interface provides different levels of geographical maps, the levels comprising world map, continental maps, local maps, individual country maps, city maps.

9. The method of any of the preceding claims, wherein the measured one or more network features for each geographical area are visualized by the graphical user interface in different graphical features..

10. The method of claim 9, wherein the graphical feature is selected from the group comprising colour, graphical pattern, flashing or combinations thereof.

11. The method of any of the preceding claims, wherein a request is an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

12. The method of any of the preceding claims, wherein geographical area is selected from the group comprising country, province, state, or city.

13. System for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising:

means for monitoring current requests to the computer system;
means for measuring one or more network features on the basis of the current requests;
display means for providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests;
an input means receiving a user input selecting at least one geographical area;
a database associating for the at least one geographical area of origin each country with corresponding IP addresses; and
means for automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

Amended claims in accordance with Rule 137(2) EPC.

1. Method of protecting a computer system from attacks over a network to which the computer system is connected, the method comprising the steps of:

a. monitoring current requests to the computer system;
b. measuring one or more network features on the basis of the current requests;
c. providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests, each of said at least one geographical area comprising at least one country
d. receiving a user input selecting at least one geographical area;
e. accessing, on the basis of the selected at least one geographical area, a database associating, for the at least one geographical area of origin, each country with corresponding IP addresses; and
f. automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

2. The method of any of the preceding claims, further comprising the step g) of filtering a sender or requests from a sender depending on the generated firewall rules for the selected at least one geographical area.

3. The method of claim 1 or 2, wherein step a) preferably also comprises accessing the database on the basis of the monitored IP addresses to retrieve therefrom information with respect to the country the monitored request is coming from.

4. The method of claim 2 or 3, wherein the step of filtering comprises of a request throttling algorithm or bandwidth throttling algorithm, wherein the limit for a particular sender corresponds to the geographical area of origin.

5. The method of claim 4, wherein the sum of all limits for all senders is selected on the basis of the server load or bandwidth usage of the computer system.

6. The method of claim 5, wherein the measured network features is selected from the group comprising: country of origin, packet rates, application features, transmission volume, estimated number of requests in a defined time interval, or combinations thereof.

7. The method of any of the preceding claims, wherein in step c) the graphical user interface comprises a geographical map.

8. The method of claim 7, wherein the graphical user interface provides different levels of geographical maps, the levels comprising world map, continental maps, local maps, individual country maps, city maps.

9. The method of any of the preceding claims, wherein the measured one or more network features for each geographical area are visualized by the graphical user interface in different graphical features..

10. The method of claim 9, wherein the graphical feature is selected from the group comprising colour, graphical pattern, flashing or combinations thereof.

11. The method of any of the preceding claims, wherein a request is an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

12. The method of any of the preceding claims, wherein geographical area is selected from the group comprising country, province, state, or city.

13. System for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising:

means for monitoring current requests to the computer system;
means for measuring one or more network features on the basis of the current requests;
display means for providing a graphical user interface visualizing the measured one or more network features for at least one geographical area of origin of requests, each of said at least one geographical area comprising at least one country;
an input means receiving a user input selecting at least one geographical area;
a database associating, for the at least one geographical area of origin, each country with corresponding IP addresses; and
means for automatically generating firewall rules for the computer system on the basis of the IP addresses retrieved from the database for the at least one selected geographical area.

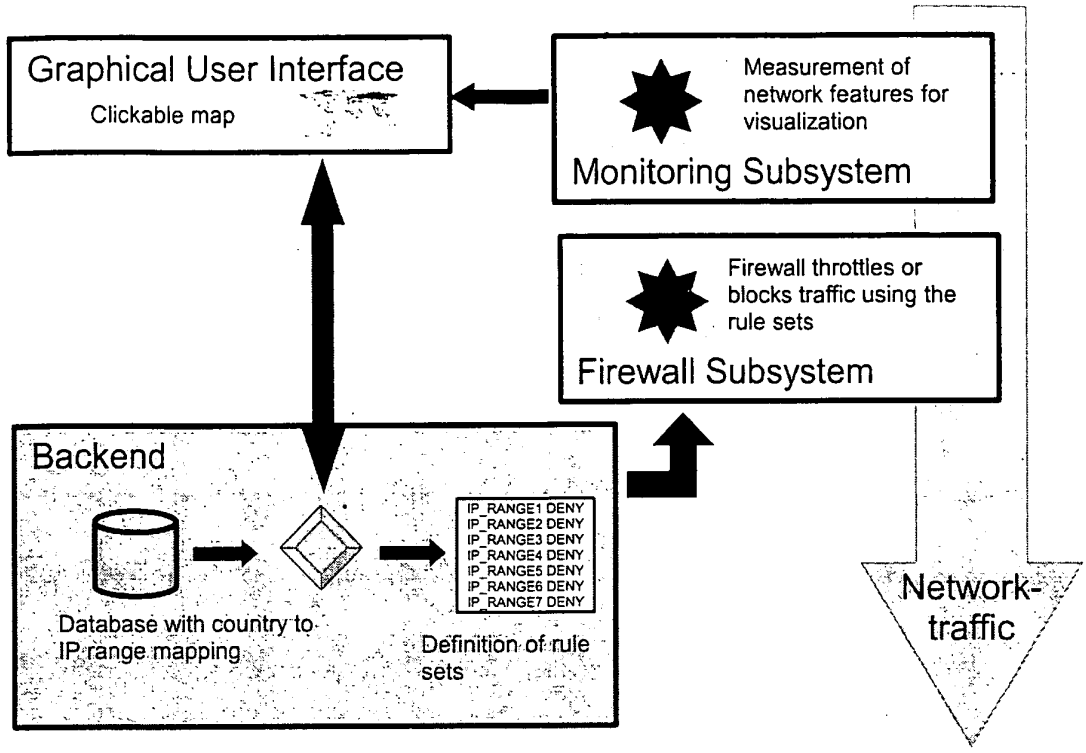
Graphical User Interface
Clickable map
Measurement of network features for visualization
Monitoring Subsystem
Firewall throttles or blocks traffic using the rule sets
Firewall Subsystem
Backend
IP_RANGE1 DENY
IP_RANGE2 DENY
IP_RANGE3 DENY
IP_RANGE4 DENY
IP_RANGE5 DENY
IP_RANGE6 DENY
IP_RANGE7 DENY
Database with country to IP range mapping
Definition of rule sets
Network-traffic

Fig. 1

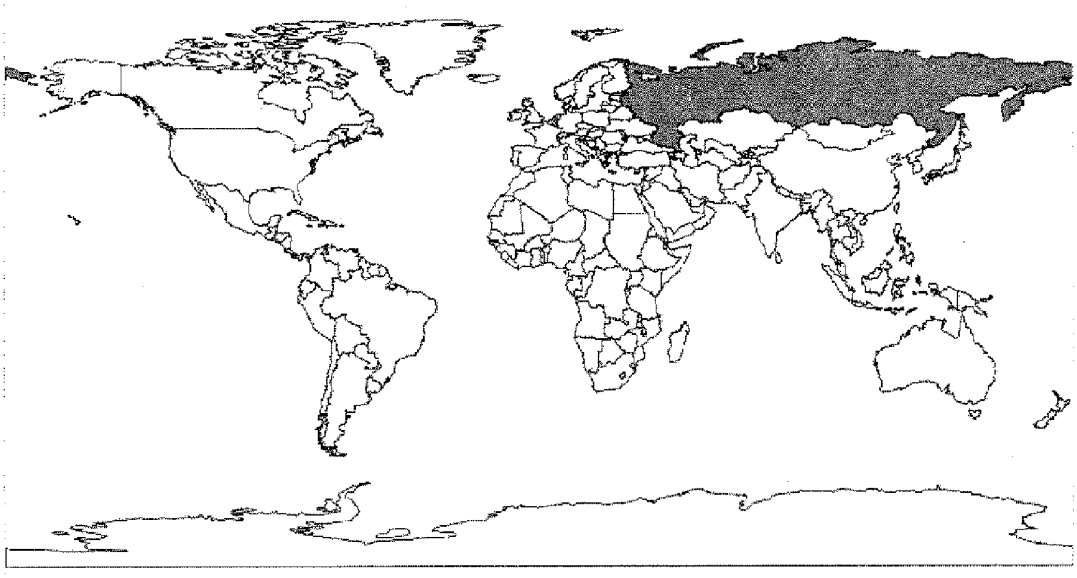

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 08 15 4391

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	US 2006/267802 A1 (JUDGE PAUL [US] ET AL) 30 November 2006 (2006-11-30) * paragraphs [0030], [0031] * * paragraphs [0061] - [0080] *	1-13	INV. H04L29/06
Y	BLOCK A COUNTRY.COM: "Blockacountry"[Online] 21 August 2007 (2007-08-21), XP002498516 Retrieved from the Internet: URL:http://web.archive.org/web/20070821043618/http://blockacountry.com/> [retrieved on 2008-10-06] * the whole document *	1-13	
Y	AZIM YASIN: "The DDOS"[Online] 20 February 2008 (2008-02-20), XP002498517 Retrieved from the Internet: URL:http://azimyasin.wordpress.com/2008/02/16/the-ddos/> [retrieved on 2008-10-06] * the whole document *	1-13	
A	US 2006/010389 A1 (ROONEY JOHN G [CH] ET AL) 12 January 2006 (2006-01-12) * paragraphs [0020] - [0022] * * paragraphs [0044] - [0047] * * paragraphs [0072] - [0074] * * paragraphs [0078] - [0096] *	1-13	TECHNICAL FIELDS SEARCHED (IPC) H04L G06F
A	J. GAUTHIER, S. SETHI, M. WEATLEY: "Geographical Event Mapping System (GEMS)" UNIVERSITY OF MANITOBA, [Online] 1 May 2006 (2006-05-01), XP002498518 Retrieved from the Internet: URL:http://gems.ee.umanitoba.ca/docs/student-final-0406.pdf> [retrieved on 2008-10-06] * the whole document *	1-13	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	7 October 2008	Olaechea, Javier

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 15 4391

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-10-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006267802 A1	30-11-2006	US 2007027992 A1	01-02-2007
US 2006010389 A1	12-01-2006	CN 1719783 A	11-01-2006
		KR 20060049821 A	19-05-2006

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **P. Ferguson ; D. Senie.** *Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing,* 2000, //rfc.net/rfc2827.html. **[0005]**
- **S. Savage ; D. Wetherall ; A. R. Karlin ; T. Anderson.** Practical network support for IP traceback. *SIGCOMM,* 2000, 295-306 **[0005]**